

Microsoft Privacy Development Standard

JC Cannon
Privacy Strategist
Corporate Privacy Group
Microsoft Corporation

Agenda

- Problem we are trying to solve
- Background of proposed solution
- How privacy development standard fits into organization
- How TCAAB can help in creation / deployment of standard

Before the Standard

- Other than Windows and Office, many product groups were building components without a privacy review
- Privacy reviews were done without regard to corporate privacy policy
- There was no consistency in how privacy reviews were performed
- No formal signoff

Purpose of the Standard

- Fulfill Microsoft's desire to build privacy-aware applications & services
- Consolidate standards and guidelines created by other product groups
- Fill void for privacy direction in product groups – once deployed

MS Privacy Development Standard

The Roadmap

Creation -----

CPG/
PG Leads

Validation --

PMC

TCAAB

Execs

Adoption -----

DMD

MSN

Office

Windows

MS Privacy Development Standard Document Creation

- Derived from corporate privacy policy
- Operationalizes PD3 philosophy
- Includes privacy work from Windows, Office, MSN, and MS.com teams
- Embraces Safe Harbor Principles

MS Privacy Development Standard

Document organization – Basic concepts

- Data classifications
 - Anonymous, PII, Sensitive PII
- Types of notice and consent
- Types of privacy controls
 - User, administrator, parental
- Data minimization
- Exception processing

MS Privacy Development Standard

Document organization – The analysis

- **Basic Privacy Analysis**
 - Determine if data is being processed
 - Provide disclosure
- **Detailed Analysis**
 - Determine component type
 - Client, service, server
 - Select type of dataflow component uses
 - Follow rules for dataflow type

Performing an Analysis

Basic Analysis



Indicate no data collected in privacy disclosure

Detailed Analysis

Select component type

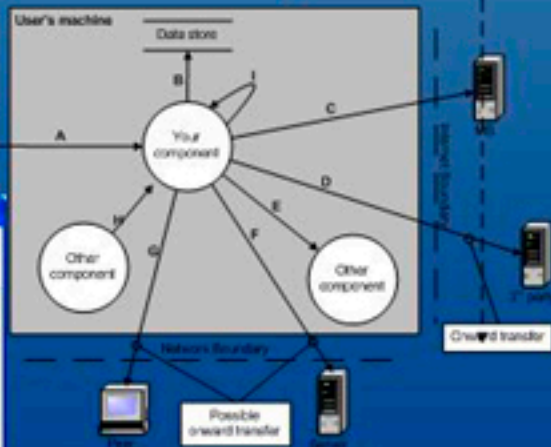
Client Component

Server Component

Service Component

Select dataflow type

- A. Collection of data from the user
- B. Transfer of data to data store
- C. Transfer of data to a Microsoft site
- D. Transfer of data to third-party sites
- E. Transfer of data to another component
- F. Transfer of data to an enterprise server
- G. Transfer of data to a peer machine
- H. Transfer of data from another component
- I. Storage of hidden data or metadata



Performing an Analysis

Basic Analysis



Indicate no data collected in privacy disclosure

Detailed Analysis

Select component type



Select dataflow type

- A. Collection of data from the user
- B. Transfer of data to data store
- C. Transfer of data to a Microsoft site
- D. Transfer of data to third-party sites
- E. Transfer of data to another component
- F. Transfer of data to an enterprise server
- G. Transfer of data to a peer machine
- H. Transfer of data from another component
- I. Storage of hidden data or metadata

Follow data processing rules

6.3 Features that transfer data from the user's computer

* MUST provide a prominent notice to users about the data that is being transferred before the data is transferred.

* MUST provide controls to permit the user to manage the transfer of the data. Management of these controls may be delegated to administrators or parents.

* MUST disable the transfer by default. That is, the user MUST be required to "opt-in" to the transfer of the data. When displaying a screen to the user with Privacy Controls, all settings that enable the transfer of data MUST be unchecked.

6.3.3 When your feature is transferring data to Microsoft

* This feature MUST be prominently disclosed, and MUST be subject to both user control and administrator control. In addition, the feature MUST provide a link to its privacy disclosure to the privacy statement of the web service that is collecting the data.

* This web service that is collecting the data should provide a privacy statement to inform the user about the data that is being collected.

MS Privacy Development Standard Status and Next Steps

Privacy Handbook



Privacy Development Standard



Eng. Excellence Guide

SDLC

Product Groups



CheckPoint Express

Engineering Excellence Guide

The screenshot shows a Microsoft Internet Explorer window titled "Planning for trustworthy computing - Microsoft Internet Explorer". The address bar shows "http://www.microsoft.com/...". The page has a blue header with "engineering excellence" and the tagline "Driving the engineering practices for building world-class products". Below the header is a navigation bar with "Home" and "Microsoft Edition". A search bar is present with the text "Search the Guide" and a "Go" button. On the left, a "Product cycle phase" sidebar lists: Planning, Design, Implementation, Stabilization, Release, As needed, About this site, FAQ, and Glossary. The main content area is titled "Planning for trustworthy computing" and includes a "Select a discipline" dropdown menu set to "Program mgmt." with a "Go" button. A link "View or print this discipline" is also visible. The text describes the four pillars of the Microsoft Trustworthy Computing (TwC) initiative, emphasizing the importance of the planning phase. A "You must" section lists several requirements for trustworthy computing.

Planning for trustworthy computing - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Links

BigWeb Excellence

engineering excellence

Driving the engineering practices for building world-class products

Home Microsoft Edition

Search the Guide

Go

Product cycle phase

- Planning
- Design
- Implementation
- Stabilization
- Release
- As needed

About this site

FAQ

Glossary

Select a discipline Program mgmt. Go

View or print this discipline

Planning for trustworthy computing

The four pillars of the Microsoft Trustworthy Computing (TwC) initiative are so important that program managers (PMs) must begin focusing on them from the very beginning, in the planning phase. Although many trustworthy computing tasks happen later in the product cycle (mainly in the design phase), you must plan to add security, privacy, reliability, and business integrity into your product from the start.

Make it your team's responsibility to ensure that customers have a safe and reliable computing experience, and that customers' personal data is protected and used properly.

You must

- Stay current with worldwide trustworthy computing issues
- Tell users how Microsoft will use their information
- Conduct privacy, confidentiality, and security reviews
- Communicate guidelines to vendors and contingent staff
- Use appropriate wording for any customer-facing content
- Follow guidelines for contests, "free," or "new"
- Assign a privacy lead to every component team

CheckPoint Express

CheckPoint Express - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links

CheckPointexpress Powered by CheckPoint

Home | Add your policy | Register your product | Contact Us | FAQs | Help Currently logged on as JC Cannon

Product Name:	Data Governance Solution (Canard) Beta-1
Executive Sponsor:	Peter Cullen (pcullen)
Product Registered By:	JC Cannon (jccannon) On 8/2/2004 8:20:15 AM
Product Released By:	

Data Governance Solution (Canard) Beta-1

+ Geopolitical (0 of 4 completed)	More Information
+ Privacy (0 of 3 completed)	More Information
+ Compliance Engineering (0 of 4 completed)	More Information
+ Security (0 of 7 completed)	More Information
+ Java Migration (0 of 1 completed)	More Information
+ Licensing (0 of 1 completed)	More Information
+ Binary Processing (0 of 2 completed)	More Information

CheckPoint Express

Privacy Requirements

CheckPoint Express - Microsoft Internet Explorer

File Edit View Favorites Tools Help

CheckPointexpress

Powered by CheckPoint

Home | Add your policy | Register your product | Contact Us | FAQs | Help

Currently logged on as JC Cannon

+ Geopolitical (0 of 4 completed) More Information

- Privacy (0 of 3 completed) More Information

☐ There is a link within your product to a privacy statement or other privacy information applicable to this product.

- Note: products that do not collect any personal information do not need to create a privacy statement. Products that wish to claim this exemption must have approval by LCA.
- The privacy statement or privacy information for this product has been approved by LCA or the appropriate privacy organization within your division.
- Further information on creating a privacy statement [is available from LCA](#).

☐ Transfers of any data by this product to Microsoft are only done with express end-user consent.

- This is applicable whether or not the data contains Personally Identifiable Information (PII).
- For further information on the rules for transferring data to Microsoft, see section 7 of [the privacy handbook](#).

☐ Transfers of any data by this product to third-parties are only done with express end-user consent.

- This is applicable whether or not the data contains Personally Identifiable Information (PII).
- For further information on the rules for transferring data to third parties, see section 10 of [the privacy handbook](#).

Extending the Standard

Missing Elements & Challenges

- Integration with Software Dev Life Cycle
- Deployment Process
 - Standalone or integrated
- Add special topics:
 - Privacy for RFID Solutions
 - Location-based services
 - Guidelines for COPPA
 - Dealing with IP addresses
 - Best practices for advertising and configuration changes
 - Retention guidelines
 - SQM / CEIP

Feedback from TCAAB

- The best way to provide feedback is by sending a redline of the standard
- Questions to be answered:
 - IS PD3+C framework optimal?
 - How is the flow of the standard?
 - Does it cover the right topics?
 - What pieces are missing?
 - How do we adapt the standard over time?
 - Should each product group add their nuances or create their own standards?

